Commonwealth of Virginia

Agency Risk Management and Internal Control Standards

Published by the
Office of the Comptroller
Draft – To Be Issued Month x, 2005

This page was left blank by intention.

Table of Contents

Introduction

OVERVIEW

Current national standards for internal control and enterprise risk management are considered "best practices" for both private sector and public sector management in the United States. These nationally recognized "best practices" directly support the Commonwealth's vision and long-term objectives, as authorized by *Code of Virginia* § 2.2-2684 *et seq*. and published by the Council on Virginia's Future:[1]

Vision Statement

The third paragraph of the Commonwealth's vision statement states:

We have a responsibility to be the best-managed state in the country. To do so, we must have a focused vision, and a fiscally responsible system that provides clear, measurable objectives, outcomes and accountability, and that attracts, motivates, rewards, and retains an outstanding state workforce.

Long-Term Objective

One of the Commonwealth's eight long-term objectives is:

Be recognized as the best-managed state in the nation.

In recent years, government interest in internal control and the broader concept of "enterprise risk management" (hereafter called "ERM") has increased as governments became more complex and as citizens demanded more accountability. An effective system of internal control:

- Provides accountability for meeting program objectives,
- Promotes operational efficiency,
- Ensures the reliability of financial statements,
- Ensures compliance with laws and regulations, and
- Reduces the risk of asset loss due to fraud, waste, or abuse.

[1] *Interim Report of the Council on Virginia's Future to the Governor and the General Assembly of Virginia*, January 12, 2005, page 16.

For each agency identified in the Appropriation Act, responsibility for implementing these standards begins with the chief executive officer (agency head) and extends to everyone in the agency. Each agency head personally holds the leadership responsibility for designing and implementing an internal control program that encompasses all agency programs and activities. Each agency's chief financial officer shares this leadership role with regard to programs for financial management, compliance, and stewardship over assets, yet ultimate accountability for both finance-related and other programs lies with the agency head.

COSO STANDARDS

Formed in 1985 in response to private sector internal control scandals, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) now sets standards for ERM and internal control in the United States. COSO has issued two seminal standards documents:

- *Internal Control – Integrated Framework* (September 1992).
- *Enterprise Risk Management – Integrated Framework* (September 2004).

The 2004 ERM framework incorporates and expands on the 1992 internal control framework. The standards herein are based primarily on COSO's 2004 ERM framework.

SARBANES-OXLEY STANDARDS

In 2002, the Sarbanes-Oxley Act (SOX) was passed by Congress and signed by the President to restore trust in publicly traded companies after another surge in internal control scandals. SOX responded to internal control breakdowns at publicly traded companies that resulted in the issuance of fraudulent financial statements, in turn causing billions of dollars in losses and tens of thousands of jobs.

Management Certification Requirements

In publicly traded companies' financial statements, their chief executive officers and chief financial officers must personally certify that they:

- Know of no material misstatements.
- Designed controls so they would know of any misstatements.
- Have evaluated the effectiveness of internal controls within 90 days prior to issuance of corporate annual financial statements.
- Reported their conclusions on internal control effectiveness.
- Disclosed any significant deficiencies in internal controls.
- Disclosed any fraud involving people who have a significant role in internal control.
- Indicated any significant change in internal controls since the internal control evaluation.

Other Major Requirements

SOX contained additional requirements for financial statements, as well as requirements for each corporation to have a code of ethics:

- Annual reports must include a statement of management's responsibility for adequate internal control and financial reporting procedures.
- Annual reports must include an assessment of the effectiveness of internal control and financial reporting procedures.
- Annual reports must include a report from the external auditor on management's assessment of the effectiveness of internal controls and financial reporting procedures.
- All publicly traded companies must have a code of ethics that encompasses:
    - Honest and ethical conduct
    - Ethical handling of actual or apparent conflicts of interest.
    - Full, fair, accurate, timely, and understandable disclosure in periodic reports.
    - Compliance with applicable governmental rules and regulations.

In effect, SOX gave COSO requirements the force of law, including unprecedented criminal sanctions for fraudulent reporting. At this time, SOX does not apply to government entities. However, the public sector anticipates a future SOX-equivalent mandate. Although public sector employees do not now face SOX criminal sanctions, SOX reinforces the status of enterprise risk management as an essential, non-optional element of organizational governance.

FEDERAL GOVERNMENT STANDARDS

OMB Circular Number A-123 (*Management's Responsibility for Internal Control*) delineates COSO-like requirements for federal agencies. In response to the internal control requirements that SOX imposes on publicly traded companies, the federal government revised Circular A-123 to strengthen requirements for management assessments of internal control over financial reporting. The revised circular also requires an annual management assurance statement on internal control over financial reports.

Circular A-123 clearly indicates that Federal government agencies are subject to SOX internal control standards and clearly aligns Federal executive agency practice with both SOX and COSO. As Federal program managers begin institutionalizing these newly adopted control standards, their effect is expected to be felt by state governments through Federal grants programs. It is not clear that Federal agencies can mandate these standards for state governments through grants programs, but alignment of Federal agency requirements (A-123), private sector requirements (SOX), and professional standards (COSO) strongly suggests that the Federal government will expect grantee agencies to conform to risk management best practice concepts.

COMMONWEALTH'S *AGENCY RISK MANAGEMENT AND INTERNAL CONTROL STANDARDS*

While Virginia's internal control standards parallel COSO's *Enterprise Risk Management – Integrated Framework*, readers should clearly understand that this document conveys the Commonwealth of Virginia's standards and that it applies to all state programs. Although the terms "risk management" and "internal control" have long standing in the financial accounting and auditing disciplines, agencies should now embrace and implement these standards comprehensively across every program.

Agency heads, managers, and all other employees should first heed these standards for managing risk and maintaining internal control. The decision to follow these standards directly or adapt an alternate methodology may depend on cost-versus-benefit and other management considerations. Agency heads are responsible for departures from these standards and are expected to explain and justify any alternate methodologies used.

Subsequent sections of this manual will refer to the Commonwealth's *Agency Risk Management and Internal Control Standards* as "ARM" or as "*Standards*." These terms refer to this manual's contents, which in turn reflect the adaptation of ERM to the environment and mission of the Commonwealth of Virginia.

LIMITATIONS IN ERM STANDARDS

Each agency head should understand that, no matter how well designed and operated, effective ERM provides only reasonable (not absolute) assurance that agency objectives will be achieved. Achievement of objectives is always influenced by limitations inherent in all management processes, including:

- Faulty judgment.
- Human error.
- Collusion.
- Management override of controls.
- Limitations disclosed by cost-versus-benefit analysis.

This document provides a foundation for mutual understanding. Following its guidance, all parties should speak a common language and communicate more effectively on ERM and internal control. Agency leaders should use this document and its embedded tools (appearing as numbered exhibits) to assess their own ERM programs against best practices, and then strengthen internal control to support the achievement of agency objectives and public policy. Future ERM activities can build upon the base established during initial implementation and strengthen ongoing strategic planning and management.

Enterprise Risk Management Defined and Described

OVERVIEW

For every planned objective, there is some risk that "things won't work as planned." This applies to operational plans as well as strategic plans. As agencies devise plans and related objectives, each objective carries risks of unwelcome or unexpected outcomes. Rather than develop strategic plans and hope that nothing will occur to prevent success, "best practice" calls for managing major risks associated with each organizational objective. ARM can help an agency to reach its objectives while avoiding pitfalls and surprises along the way.

Readers should note that ARM does not change either strategic plans or the strategic planning process. ARM uses objectives, already developed by the current strategic planning process, but does not alter the planning process itself.

"Enterprise Risk Management" is a comprehensive and systematic program to identify, measure, prioritize, and respond to the risks associated with reaching organizational objectives.

ARM should not be viewed as "something added" to an agency's management activities. Instead, ARM should be an integral part of strategic and operations planning. Integrated ARM converts reactive management into proactive management, and can help avoid unnecessary procedures and costs.

Code of Virginia § 2.2-5511 requires agencies to develop strategic plans. The Virginia Department of Planning and Budget issues guidelines for strategic planning, service area planning, and performance – based budgeting.

The strategic plan serves as a key management tool for agency leaders as they oversee performance and make course corrections to ensure the agency reaches its strategic goals.

All components of the strategic planning process (mission statement, values, goals, objectives, measures, strategies) form the foundation for an ARM program.

GLOSSARY

Glossary

Agency

In these *Standards*, "agency" refers to any unit of government identified by an agency number in the Appropriation Act. "Agency" includes every state department, division, officer, board, commission, institution or other unit of state government.

These *Standards* are mandatory only for agencies in the Executive branch of government. Application by other governmental branches and entities is encouraged.

Agency Head

The chief executive officer of an agency, as "agency" is defined in this section.

"ARM"

Refers to "*Agency Risk Management and Internal Control Standards*" as embodied in this manual. ARM reflects the adaptation of ERM concepts to the Commonwealth of Virginia's agencies.

ARM Components

Same as "ERM Components," subsequently defined in this glossary.

***Code of Virginia* or "Code"**

The Commonwealth's statutes as codified in the *Code of Virginia of 1950* (as amended).

Control Activities

Policies and procedures established and implemented to help ensure the risk responses are effectively carried out. Control activities occur throughout an organization, at all levels, and in all functions. They include:

- Review and approval.
- Authorization.
- Verification.
- Reconciliations.
- Physical security over assets.
- Segregation of duties.
- Education, training, and coaching.
- Performance planning and evaluation.

Enterprise Risk Management or "ERM"

Process headed by agency head, applied agency-wide in strategic planning, identify potential events and provide reasonable assurance regarding the achievement of strategic objectives. **ERM does not replace internal control; ERM <u>includes</u> internal control.**

Glossary

ERM Components

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

Event Identification Process of identifying potential internal and external events that could affect achievement of agency objectives. Agency management must identify these events and determine whether they represent risks or opportunities. Risks have a negative impact and require management's assessment and response. Opportunities are channeled back to management's strategy or objective-setting processes.

Information and Communication Communicating relevant information in a timeframe to enable people to carry out their responsibilities. Effective communication occurs down, across, and up the agency.

An effective information and communication process ensures that all personnel receive a clear message from the agency head that risk management must be taken seriously.

Inherent Risk The risk that one or more factors will prevent an objective from being accomplished, if the agency does nothing to ensure that objective is accomplished.

Internal Control Ongoing process led by agency head to design and provide reasonable assurance that these types of objectives will be achieved:

- Effective and efficient operations
- Reliable financial reporting
- Compliance with applicable laws and regulations
- Safeguarding of assets

Internal Control Components

- Control Environment
- Information and Communication
- Assessment and Management of Risk
- Control Activities
- Monitoring Activities

Glossary

Internal Environment

The agency's "corporate culture," showing how much the agency's leaders value ethical behavior and internal control. Factors include:

- Values stated and promoted for integrity and ethical behavior,
- Commitment to competence,
- Organizational structure,
- Assignment of authority and responsibility,
- Human resource standards,
- Risk management philosophy,
- Risk appetite,
- Oversight by the Cabinet Secretary, and
- Oversight by the agency's board or commission (when applicable).

Monitoring

The process of assessing the presence and functioning of risk management components, and making continuous improvements. Monitoring can be accomplished by routine management activities, separate evaluations, or both.

Objective

Description of the results that, when achieved, move an organization toward its stated goals. There can be any number of objectives associated with a goal. An objective could have one or more of the following key characteristics.

- Describes results needed to accomplish the goal.
- Is measurable.
- Begins (usually) with an action verb.
- Supports multiple initiatives or strategies.
- Collectively addresses key programs or functional areas.

A specific example: *Promote self-sufficiency*.

(Adapted from DPB's agency *Planning Handbook – A Guide for Agency Strategic Planning and Service Area Planning Linking to Performance-Based Budgeting*, May 1, 2005)

Objective Setting

An integral part of strategic planning. Strategic level objectives provide a basis for setting operational, reporting, and compliance objectives. Objectives must be established before agency heads can effectively identify events, assess risk, and establish risk responses. Agency risk management relies on objectives that:

- Support the agency's mission and
- Have tolerable risk levels.

Residual Risk

The risk that remains after management responds to inherent risk. Once risk responses have been developed, management then considers residual risk.

Glossary

Risk Appetite The amount of risk an agency accepts in pursuit of its objectives. (While an agency may decide to accept more or less risk in pursuit of its programs' objectives, the agency head is not authorized to accept risk that would jeopardize the agency's financial reporting and compliance objectives.)

Risk Assessment Process of analyzing potential events and determining what impact they may have on achieving agency objectives.

Risk Response The choice that management makes in response to risk, chosen from these options:

- Avoid risk.
- Reduce risk.
- Share risk.
- Accept risk.

Risk Tolerances Acceptable levels of variation from ideal results in meeting objectives.

ROLES AND RESPONSIBILITIES

Each state employee has individual responsibility for risk management. The agency head is ultimately responsible and must assume ownership. Other agency executives and managers must support the agency's risk management philosophy, promote compliance, and manage risks within their scopes of responsibility, consistent with risk tolerances. The risk officer, chief financial officer, internal auditor, and others usually have key support responsibilities. Other agency personnel are responsible for supporting risk management according to laws, directives, policies, procedures, and their agency's code of ethics.

External parties such as citizens, customers, the General Assembly, other agencies, outside auditors, and regulators often provide information that is useful in effecting ARM. However, external parties are neither responsible for nor part of an agency's risk management program.

EMPHASIS ON SOFT CONTROLS

The ERM framework emphasizes "soft control" activities. Traditionally, internal control systems focused on "hard" controls (such as physical or electronic controls). Soft controls are intangibles that management emphasizes to direct the organization.

Soft Controls

Underlying Drivers

- Integrity
- Ethical values
- Philosophy
- Operating style
- Communication principles
- Commitment to competence
- Commitment to performance
- Commitment to public policy
- Commitment to risk management

Examples of Soft Controls

- Performance incentives
- Performance standards used for hiring and promotion
- Employee training and education programs
- Encouragement of new ideas and methods
- Periodic employee feedback and interview sessions
- Analysis of and response to customer and supplier feedback
- Review and investigation of exception reports
- Effective employee suggestion programs

Agency Risk Management and Internal Control Standards

OVERVIEW

Virginia has designed these *Standards* to achieve five objectives.

1. Strategic – high-level goals and objectives, aligned with and supporting the mission.
2. Operational – effective and efficient use of resources.
3. Reporting – integrity and reliability of reporting.
4. Compliance – compliance with applicable laws and regulations.
5. Stewardship – protection and conservation of assets.

To meet Virginia's *Standards*, an agency must demonstrate that it has eight risk management components established and fully functioning:

1. Internal environment.
2. Objective setting (as part of strategic and operational planning).
3. Event identification.
4. Risk assessment.
5. Risk response.
6. Control activities.
7. Information and communication.
8. Monitoring.

Agency size, complexity, programs, "corporate culture," management style, and other attributes will affect how these *Standards* are effectively and efficiently implemented. Even with these and other variables, the following stages usually occur when creating an ERM program.

ERM Implementation Steps	
Preparedness	Name a core team representing organizational units, key support functions, and strategic planning. This team becomes intimately familiar with framework components, concepts, and principles.
Executive Sponsorship	Executive support drives success. Executive sponsorship must be visible early and often.
Implementation Planning	Write an implementation plan. The plan should set out project phases, work streams, milestones, resources, deadlines, and responsibilities. Put a project management process in place. During subsequent steps, revise the plan as appropriate.

ERM Implementation Steps	
Assessment of Current Status	Assess how risk management components, concepts, and principles currently are applied across the agency. Identify whatever risk management philosophy has evolved in the agency. Determine the agency's risk appetite, remembering that risk appetite may not jeopardize meeting an agency's financial reporting or compliance objectives.
Risk Management Vision	Develop a vision for how risk management will be integrated into the DPB-mandated process for program planning, budgeting, management, and evaluation.
Capability Development	Use the *Current State Assessment* and the *Risk Management Vision* to determine the people, technology, and process capabilities already in place and functioning, as well as new capabilities that need to be developed.
Change Management	Take action to complement and sustain the agency risk management vision and desired capabilities – develop deployment plans, training sessions, reward reinforcement mechanisms, and monitoring processes for the remainder of the implementation process.
Monitoring	As part of the ongoing management process, continually review and strengthen risk management capabilities.

To help agencies meet these *Standards*, specific techniques for applying the concepts and principles in each of the components of the ARM framework follow. Other resources:

- Appendix A: Sample tools for implementing and documenting the agency risk management process.

- Appendix B: Sample tools for evaluating internal controls, a prerequisite to signing the certification regarding internal controls.

- COSO's *Enterprise Risk Management – Integrated Framework* is available from:

    - www.coso.org/publications/erm/coso_erm_executivesummary.pdf – for free download of the framework's *Executive Summary*.

    - www.cpa2biz.com/cs2000/products/cpa2biz/publications/coso+enterprise+risk+management+-+integrated+framework.htm for purchasing the entire framework.

INTERNAL ENVIRONMENT

All other ARM components stand on an "Internal Environment" foundation. The internal environment reflects top management's expectations for how seriously agency employees should view and manage risk.

Internal environment is extremely important and has major impact – positive or negative – on ARM programs. The attitude and concern that top management expresses for effective ARM must be definitive and clear, and must permeate the agency. Stated support is not sufficient – words must be reflected in executive action and demeanor.

Risk Management Philosophy

An agency's risk management philosophy is the set of shared beliefs and attitudes characterizing how the agency considers risk in everything it does, from strategy development and implementation to its day-to-day activities. Risk management philosophy reflects the agency's values, influencing its culture and operating style, and affects how ARM components are applied, including how risks are identified, the kinds of risks accepted, and how they are managed.

Risk management philosophy is captured in policy statements, oral and written communications, and decision-making. Management reinforces the philosophy not only with words but also with everyday actions.

Risk Appetite

Risk appetite is the amount of risk, on a broad level, that an agency is willing to accept in pursuit of its programmatic objectives. It reflects the agency's risk management philosophy, and in turn influences the agency's culture and operating style, in programs that provide direct services to others, including citizens, regulants, clients, elected officials, and other agencies.

State agencies may consider risk appetite qualitatively, with such categories as high, moderate, or low. Or they may consider risk appetite quantitatively by reflecting and balancing goals for growth and return with risk.

As chief executives of government agencies, agency heads are not authorized to take risks that would knowingly jeopardize their ability to meet obligations for financial management and reporting or compliance with laws, regulations, policies, and procedures. Financial reporting and compliance objectives serve needs of both the agency and of the Commonwealth as a whole, and are "not negotiable" when choosing strategies or tactics for achieving program objectives.

Oversight by the Agency's Board

An agency's board (commissioners, visitors, or directors) plays a critical part in the internal environment and significantly influences its elements. The board's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and appropriateness of its actions all play a role. Effective boards require effective ARM programs.

Integrity and Ethical Values

An agency's strategy, objectives and implementation stem from preferences, value judgments, and management styles. Management commitment to ethics influences these preferences and judgments, which translate into behavioral expectations. ARM effectiveness cannot rise above the integrity and ethical values of the people who create, lead, and monitor agency programs. To protect an agency's reputation, standards of behavior must exceed mere compliance with law. Top agencies reflect a belief that good ethics is good government.

Work Force Competence

Competence reflects the knowledge, skills, and abilities needed to meet objectives. Management sets competencies for particular jobs and translates those competencies into *Employee Work Profiles* and employee development programs.

Assignment of Authority and Responsibility

Assignment of authority and responsibility involves the degree to which individuals and teams are authorized and encouraged to use initiative to solve problems. It includes establishing reporting relationships, fixing authorization procedures, issuing policy that assign appropriate personnel to each program, and allocating resources to do each job. A critical challenge is delegating to the extent required to achieve objectives, ensuring that decision making is based on sound practices for risk identification and assessment. Another challenge is ensuring that everyone understands objectives and how his or her job contributes to meeting those objectives.

Organizational Structure

An agency's organizational structure provides the structure to plan, execute, control, and monitor activities. A sound organizational structure defines key areas of authority and responsibility, while illustrating reporting lines. An organizational structure may be centralized or decentralized; it may create direct reporting lines or a matrix format. An agency may be organized by services, geographical locations, or enabling statutes.

Human Resources Development

Human resources practices for hiring, orientation, training, evaluating, counseling, promoting, compensating, and remediation send messages to employees about expectations for integrity, ethical behavior, and competence. For example, standards for hiring and retaining the most qualified and ethical individuals demonstrate an agency's true culture. Providing continuing training and education can reward expected performance and behavior. It is essential that employees be groomed to tackle new challenges as agencies become ever more complex.

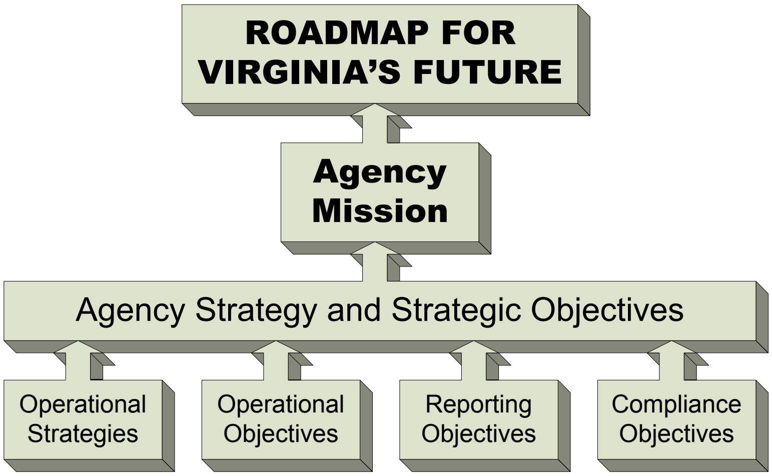
OBJECTIVE SETTING

"Objective Setting" is the process of identifying objectives at a strategic level. Strategic level objectives provide a basis for then setting operational, reporting, and compliance objectives. Objectives must exist before management can effectively identify events, assess risk, and establish risk responses. ARM ensures that management has a process in place to set objectives, chosen objectives support and align with the agency mission, and objectives are consistent with risk appetite.

Strategic Objectives

Strategic objectives stand at the top level of importance, align with and support the agency mission, and must align with and support the Commonwealth's objectives, found in the *Roadmap for Virginia's Future*. An agency's mission sets out what the agency aspires to achieve in the broadest sense. To support its mission, the agency sets strategic objectives, formulates strategy, and establishes related operations, reporting, and compliance objectives. While an agency's mission and strategic objectives are generally stable, its strategy and many related lower level objectives are more dynamic, changing with internal and external conditions. As needs change, strategy and objectives are realigned with strategic objectives.

Alignment of Agency Strategic Plan with the Statewide Plan



Aligning operations to support both agency and public policy objectives is critical to success. Setting objectives at the agency and operating levels will reveal critical success factors, the key "things that must go right" if goals are to be attained. Critical success factors are defined for agency, division, department, and person as managers sequentially choose:

- Agency strategy
- Agency objectives
- Unit strategies
- Unit operations, reporting, and compliance objectives.

While establishing unit objectives, managers should identify performance criteria that will tie to *Employee Work Profiles* and other performance assessments of individuals and work units.

Operations Objectives

Operations-level objectives pertain to effective and efficient agency performance, meeting performance goals, and safeguarding resources against loss. They reflect management's choices about structure and performance. Management must ensure that the objectives reflect reality and the demands of the stakeholders, while continuing to link with the agency strategic plan and statewide plan. Operations objectives provide a focal point for allocating resources; unclear or ill-conceived objectives can misdirect resources.

Reporting Objectives

Reporting objectives pertain to reliability and information integrity. They cover internal and external reports and involve both financial and non-financial information. Reporting should support management decision-making and monitoring of the agency.

Compliance Objectives

Compliance objectives enforce adherence to relevant laws, regulations, policies, and procedures. They depend largely on external factors and tend to be similar across all agencies. For agencies, they typically relate to relevant federal, state, and local law, regulations, policies, procedures, grants, and contracts, as well as agency management prerogatives.

Other Issues Related to Objectives

An agency's categorization of objectives is not limited to categories named in this document. An agency may develop a subset of an ARM category to facilitate communication on narrower topics. Also, an objective in one category may overlap or support an objective in another. In order to have assurance that all categories of objectives are being met, all eight of the ARM components must be functioning in support of the objectives.

ARM Impact on Reporting and Compliance

Since achieving reporting and compliance objectives is largely within the agency's control, ARM can provide reasonable assurance that those objectives are being achieved. However, external events beyond an agency's control may interfere with that agency's ability to meet its objectives. ARM can provide reasonable assurance that executives receive timely status reports on achieving strategic and operations objectives.

Risk tolerances are the acceptable levels of variation related to achieving objectives. Risk tolerances can be measured, often best measured in the same units as related objectives. When setting risk tolerances, managers consider the relative importance of objectives and align risk tolerances with risk appetite, giving comfort that the agency will achieve its objectives.

EVENT IDENTIFICATION

"Event Identification" lists potential internal and external events that could affect achievement of an agency's objectives. Management must identify these events and determine whether they represent risks or opportunities. Risks have negative impact and require management assessment and response. Opportunities may have positive impact and are channeled back to management's strategy or objective-setting processes.

Events range from the obvious to the obscure; events' impacts range from inconsequential to severe. To avoid overlooking relevant events, identify all events before assessing the likelihood of occurrence or impact. If potential impact is great, even consider events with a very low possibility of happening. Begin by considering a range of potential events without focusing on whether the impact is positive or negative. This way, management identifies not only potential events with negative impact, but also those representing opportunities to be pursued.

External Events

External events include economic, natural environment, political, social, and technological news. Economic events include recessions, when tax revenues drop and funding shrinks. Natural events such as hurricanes or floods may restrict service delivery and destroy infrastructure. Political events such as gubernatorial elections alter public policy and set new priorities. Social events include potential terrorist activity that creates demand for specialized services. Technology events include new electronic commerce services that change citizen expectations.

Internal Events

Internal events stem from management choices about how the agency will run. These events include infrastructure, personnel, process, and technology. Infrastructure events could include budget reallocations to meet new demands. Personnel events could include absence of key employees, new hires, terminations, and retirements. Process events could include process changes without adequate change management steps, or process execution errors. Technology events include information system downtime, security breaches, and fraudulent transactions.

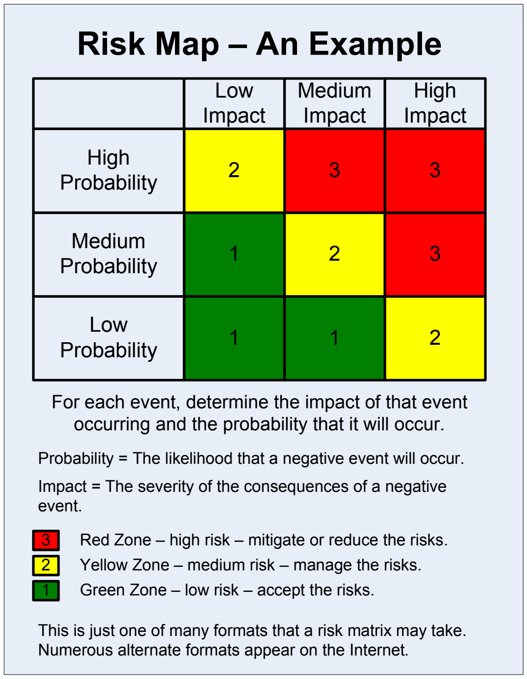
Event identification can use a combination of techniques, together with supporting tools. Event identification techniques look to both past and future; techniques include event inventories, internal analysis, escalation or threshold triggers, facilitated workshops and interviews, process flow analysis, leading event indicators and loss event data methodologies.
Internal analysis may occur as part of routine planning and performance reporting, sometimes in staff meetings. Facilitated workshops and interviews can uncover events by drawing on accumulated expertise of employees and other stakeholders. Process flow analysis considers the combination of inputs, tasks, responsibilities, and outputs that forms a process, and then identifies events that could affect achievement of process objectives. Leading event indicators

derive from data correlated to events (such as economic indicators foreshadowing bull markets). Loss event data (such as insurance claims) methodologies rely databases of past individual loss events; this could identify trends and root causes.

Often, events do not occur in isolation. One event can trigger another, and events can happen concurrently. It may be useful to group potential events into categories. By aggregating events horizontally across an agency and vertically within divisions or departments, management can develop an understanding of relationships between events, gaining enhanced information as a basis for risk assessment. By grouping similar events, management can better determine opportunities and risks.

RISK ASSESSMENT

> **"Risk Assessment" is the process of analyzing potential events, considering likelihood and impact, as a basis for determining what impact they may have on the achievement of objectives. Risks are assessed on an inherent and a residual basis.**



Risk Map – An Example

	Low Impact	Medium Impact	High Impact
High Probability	2	3	3
Medium Probability	1	2	3
Low Probability	1	1	2

For each event, determine the impact of that event occurring and the probability that it will occur.

Probability = The likelihood that a negative event will occur.

Impact = The severity of the consequences of a negative event.

- 🟥 3 Red Zone – high risk – mitigate or reduce the risks.
- 🟨 2 Yellow Zone – medium risk – manage the risks.
- 🟩 1 Green Zone – low risk – accept the risks.

This is just one of many formats that a risk matrix may take. Numerous alternate formats appear on the Internet.

In risk assessment, management considers the mix of potential events relevant to the agency and its activities in the context of the agency's risk profile, which includes size, operations complexity, and regulatory restraints. Management must consider both expected and unexpected events. Many events are routine, recurring, and already addressed in management's programs and its operating budgets. Management must assess the risk of unexpected potential events and any expected events that could have a significant impact. Risk assessment is a continuous and repetitive interplay of actions occurring throughout an agency.

Management should assess events from two perspectives – likelihood and impact – and use a combination of both qualitative and quantitative methods. The positive and negative impacts of potential events should be examined individually or by category. A visual matrix can be used to categorize events by risk level. Risks should be assessed on both an inherent and residual basis.

- **Inherent risk** is the risk to an agency if management takes no action to reduce either likelihood or impact.

- **Likelihood** is "the odds" that a given event will occur.

- **Impact** is a measurement of effect, in quantitative or qualitative terms.

- **Residual risk** is the risk that remains after management's risk response.

Often, likelihood and impact estimates are based on past events, offering some objectivity. Management first assesses inherent risks. Once a risk response is chosen, management then assesses residual risk.

RISK RESPONSE

"Risk Response" is how management chooses to respond to risk from among four options: avoiding, reducing, sharing or accepting risk. Management develops a set of actions to align risks with the agency's risk tolerances and risk appetite.

- **Avoidance** means ending those activities that give rise to risk (for example, eliminating a service or division).

- **Reducing** can apply to likelihood, impact, or both. This involves everyday management decisions. For example, routine mechanical maintenance could decrease the likelihood of a major computer hardware failure, while routine backups could decrease the impact of technology equipment failure on the agency's ability to provide services.

- **Sharing** transfers a portion of likelihood or impact to another party. Examples of sharing include acquiring insurance or outsourcing an activity.

- **Acceptance** means taking no action in response to risk, within parameters dictated by state policy. All risk cannot be eliminated, so some risk is accepted without avoidance, reduction, or sharing.

In considering its response, management should consider such factors as:

- The effect on likelihood and impact.

- The response options that align with the agency's risk tolerances.

- Cost-versus-benefit – When considering cost-benefit and recognizing interrelationships among risks, management can pool agency risk responses across subdivisions.

- Possible opportunities created by the risk responses.

Management typically considers risk for each department or major activity, with a responsible manager developing a composite assessment for each unit or major activity. Then, viewing risks for all units and major activities, senior management is positioned to take an agency-wide view and determine whether the agency's residual risk is within its overall risk appetite.

Risks in different units or activities may be within their respective managers' risk appetites but, taken together, may exceed the agency-wide risk appetite. In such cases, additional or different responses are needed to bring risk within the agency's risk appetite. Conversely, risks may naturally offset across an agency; for example, some units might have higher risk while others remain relatively risk-averse, such that overall risk is within the agency's risk appetite.

An agency-wide view of risk can be depicted in a variety of ways, such as

- Major risks,
- Event categories across departments, or
- Risk for the agency as a whole.

When viewing risk agency-wide, management can reevaluate the nature and type of risk it wishes to take. If agency-wide risk is significantly less risk than the agency risk appetite, management may decide to enhance program services by accepting greater risk in targeted areas.

CONTROL ACTIVITIES

"Control Activities" are policies and procedures implemented to help ensure that risk responses are effectively completed. Control activities occur across an organization, at all levels, and in all functions. They include a range of activities such as approvals, authorizations, verifications, reconciliations, security over assets, and segregation of duties.

Control activities can be categorized based on the nature of the objectives to which they relate: strategic, operations, reporting, and compliance. Sometimes, control activities satisfy agency needs in more than one category. They provide reasonable assurance that objectives are being achieved in strategy setting, effectiveness and efficiency of operations, reliability of financial reporting, and compliance with laws and regulations. When management selects risk responses, management identifies control activities needed to help ensure that the risk responses are executed properly and on time. In some cases, a single control activity will address multiple risk responses. In other cases, multiple control activities will apply to one risk response. Managers should consider control activity cost-versus-benefit.

Sometimes, the control activity **is** the risk response. For example, if the objective is to ensure that transactions are properly authorized, the response will likely be control activities such as segregation of duties and approvals by supervisory personnel.

Types of control activities include preventive, detective, manual, computer, and management controls. Control activities can correspond to specified control objectives, such as ensuring completeness and accuracy of data processing. The following list describes commonly used control activities, although it is not all-inclusive.

- **Top-Level Reviews** – Agency executives review actual performance versus plans, budgets, forecasts, and prior period accomplishments. Major initiatives are tracked and plan execution is monitored.

- **Direct Management** – Managers running functions or activities review performance reports and reconciliations performed.

- **Information Processing** – A variety of automated controls check data completeness, accuracy, and authorization.

- **Physical Controls** – Equipment, inventory, securities, cash, and other assets are physically secured, then periodically counted and compared with control records.

- **Performance Indicators** – Comparing different sets of data (operational or financial) to one another, analyzing data relationships, and taking investigative and corrective actions serves as a control activity. By investigating unexpected results or unusual trends, management may find circumstances where an objective appears less likely to occur than expected. An example of a performance indicator is staff turnover by unit or employee class.

- **Segregation of Duties** – Duties are divided, or segregated, among different people to reduce the risk of error or fraud. Error or fraud is easier to conceal when one person acts alone. Segregated duties require more than one person to complete a process, making it more likely that an error or fraud will be detected.

Often, a combination of controls deals best with related risk responses. Control activities include preventive controls to stop certain transactions before execution, and detective controls to identify other transactions on a timely basis. The control activities combine computer and manual controls, including automated controls to ensure all information is correctly captured, and routing procedures enabling responsible individuals to authorize or approve decisions.

Control activities usually involve two elements: first policy establishes standards, and then procedures effect policy. Policies must be implemented thoughtfully and consistently. Conditions identified by control procedures should be investigated and appropriately handled.

Control Activities over Information Systems

General controls include controls over information technology management, infrastructure, security management, and software acquisition, development, and maintenance. For example:

- **Information Technology Management** – A steering committee oversees, monitors, and reports on information technology activities and improvement initiatives.

- **Information Technology Infrastructure** – Controls apply to system definition, acquisition, installation, configuration, integration, and maintenance. Controls include continuity of operations (COOP) planning, scheduling computer operations, restricting access to system configuration and operating system software, incident tracking, system logging, and monitoring use of data-altering utilities.

- **Security Management** – Secure passwords restrict internal access to the network, database, and applications. Firewalls and virtual private networks protect data from unauthorized external access.

- **Software Acquisition, Development, and Maintenance** – Software acquisition and implementation controls are incorporated into a formal change management process. One control over development is allowing software developers to work only in segregated development environments with no access to the production environment. System change controls include authorizations, reviews, approvals, documentation, and testing.

Application controls focus directly on capture and processing of complete, accurate, authorized, and valid data. They help ensure data are captured or generated when needed, supporting applications are available, and interface errors are corrected quickly. Application controls help to prevent, detect, and correct errors. Controls (including edit checks for format, existence, reasonableness, and validity) are built into application software. Examples follow.

- **Balancing and Reconciling** – Reconciling amounts entered to a control total will help detect data capture errors.
- **Check Digits** – Check digit logic helps detect and correct incomplete or inaccurate data.
- **Predefined Data Listings** – For example, using drop-down lists of acceptable values.
- **Data Reasonableness Tests** – Data captured is compared with a benchmark.
- **Logic Tests** – Range limits, value, or alphanumeric tests can detect potential errors.

INFORMATION AND COMMUNICATION

"Information and Communication" involves identifying, capturing and communicating relevant information in a form and timeframe that enables people to carry out their responsibilities. Effective communication occurs down, across, and up the agency. An effective information and communication process will assure that all personnel receive a clear message from top management that ARM responsibilities must be taken seriously.

An entire agency needs **information** to handle risks, provide services, and achieve objectives. Quantitative and qualitative information comes from many internal and external sources. Information enables change management, strategy, identifying events, analyzing risks, picking risk responses, and carrying out other management activities.

Information systems architecture and technology acquisition are key elements of strategy. IT selection and implementation depends on many factors, including organizational goals and stakeholders' service expectations. Information systems are fundamental to ARM; in turn, risk management techniques assist in making technology decisions. Usually, IT infrastructure developed over time to support operations, reporting, and compliance objectives also generate information integral to the ARM program.

IT infrastructure should capture timely, detailed, and reliable data sufficient to feed ARM. Timely information flow must keep pace with change in the agency's environment, while avoiding "information overload" or "paralysis by analysis."

Communication is inherent in information systems but also must take place in a broader sense, dealing individual and group responsibilities and expectations. Information must be conveyed so that people can do their jobs.

Clear **internal communication** conveys the agency's code of ethics, risk management philosophy and approach, and delegated authority. Communication about processes and procedures should support the mission and agency culture. Communication should effectively impart the importance and relevance of ARM and the roles each person plays to support it.

Front-line employees providing direct daily public service are often in the best position to see new problems as they arise. Communication channels should ensure that front-line and other personnel can communicate risk-related information across divisions and processes, as well as to their managers. Communication breakdowns can occur when anyone is discouraged from or unable to provide important information to others.

To avoid breakdowns, personnel must believe managers and agency heads truly want to know about problems and resolve them. Usually, normal agency reporting lines are the appropriate channels for communication. Sometimes, alternate communication lines are needed as a fail-safe mechanism if normal channels do not work. The Commonwealth's "Fraud, Waste, and Abuse Hotline" is one such alternate channel. This hotline provides a ready means for any employee to confidentially discuss illegal, unethical, or otherwise inappropriate behavior.

Critical communications channels lie between the agency head and cabinet secretary, and the agency's board or commission (when one exists). The better the communications to appointed officials, the more effective they can be in meeting their oversight responsibilities.

Open **external communication** channels allow citizens, clients, and suppliers to provide valuable input on services quality and design. This enables an agency to address evolving needs, demands, and preferences. Management should appropriately convert such input into continuous improvements in operations, reporting and compliance. Open external communications also allow citizens and clients to understand the agency's service standards.

Communication vehicles can take such forms as a **Code of Ethics**, Internet sites, policy manuals, memos, e-mails, and posted notices. Whenever messages are transmitted orally – in large groups, smaller meetings, or one-on-one sessions—tone of voice and body language emphasize what is being said.

Personnel management style sends a powerful message. Managers should remember that actions speak louder than words. Their actions are, in turn, influenced by the agency's history and culture, drawing on past observations of how their mentors dealt with similar situations.

MONITORING

"Monitoring" is the process of assessing the presence, functioning, and continuous improvement of ARM components. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Monitoring can be done in two ways: through ongoing activities or separate evaluations. If ARM mechanisms are structured to monitor themselves on an ongoing basis, there may be less need for separate evaluations.

Ongoing monitoring is built into normal, recurring operating activities, is performed on a real-time basis, reacts dynamically to changing conditions, and is ingrained in the agency. Ongoing monitoring often stems from regular management activities, which might involve analysis, comparison of information from disparate sources, and dealing with unexpected occurrences.

Line operating or functional support managers, giving thoughtful consideration to implications of information they receive, generally perform **ongoing monitoring activities**. By focusing on relationships, inconsistencies, or other relevant observations, they identify issues and follow up with others to determine whether or not action is necessary. (Activities required by operational processes are generally not considered monitoring activities. For example, approvals of transactions, reconciliations of account balances, and verifying the accuracy of changes to master files, performed as required steps in information systems or accounting processes, are best defined as control activities.) Examples of ongoing monitoring activities include:

- Managers reviewing operating reports.
- Internal auditors, external auditors, and advisors regularly providing recommendations.
- Training seminars, planning sessions and other meetings designed for feedback to management.

In addition to ongoing monitoring activities, it may be useful to take a fresh look from time to time, focusing directly on ARM through **ad hoc evaluations**. These provide an opportunity to consider the continued effectiveness of the ongoing monitoring procedures. Direct evaluations are control self-assessments, where persons responsible for a particular unit or function determine the effectiveness of ARM for their activities. Internal auditors perform evaluations as part of their regular duties or by specific request of senior management. Management may use input from external auditors. A combination of efforts may be used in conducting whatever evaluation procedures management deems necessary to determine the effectiveness of ARM. Tools used to monitor may include checklists, questionnaires, and flow charts.

Ongoing Monitoring vs. Ad Hoc Evaluations

	Monitoring Ongoing Operations	Ad Hoc Evaluations
Focus	Routine management and supervision of programs and personnel.	ARM in one or more units or programs.
ARM Emphasis	One of many factors being monitored.	The primary factor being investigated and analyzed.
Reporting	Significant findings likely to appear in periodic, routine management reports (for example, monthly manager's report to the agency head). Less-than-significant findings may not appear in formal reports.	A "special project" report prepared by management, agency internal auditor, agency inspector general, APA, JLARC, State Internal Auditor, consultant, or other.

ARM documentation varies with agency size, programs, budget, employment level, and similar factors. The first component includes existing policies and procedures issued by central agencies (DOA, DPB, Treasury, VITA, DGS, DHRM, Library of Virginia, etc.), policies and procedures published within the agency, and applicable federal regulations (for example, IRS regulations and federal grant requirements). A review of existing documentation should clearly describe an agency's or unit's risks and responses. Documentation takes these forms:

Control Activity Documentation – Some Examples

- Budget-to-actual and exception reports
- Completed *Authorized Signatories* forms
- Completed *Employee Work Profile* forms
- Delegations of authority
- Descriptions of key roles, authorities, and responsibilities
- Format of periodic management reports
- Key identified risks
- Key performance indicators
- Key risk measures
- Operating procedures
- Organization charts
- Policies and procedures manuals
- Process flowcharts
- Relevant controls and related responsibilities
- Standardized forms (e.g., travel authorizations)
- Strategic and operational plans

The second component forms the basis for developing review processes, including tests to determine whether the processes and related policies and procedures represented are adequate and being followed. The leader of an ad hoc evaluation may develop documentation to achieve the following objectives:

- Create a history of the team's assessments and testing
- Communicate evaluation results – findings, conclusions, and recommendations
- Facilitate review by senior management
- Facilitate future evaluations
- Identify and report strategic issues
- Identify individual roles and responsibilities in ad hoc evaluation project
- Supplement existing ARM documentation

ARM deficiencies may surface from many sources including an agency's ongoing monitoring procedures, ad hoc evaluations, and information provided by external parties. External sources include customers, vendors, external auditors, and regulators. All identified deficiencies that affect the agency's ability to implement its strategy and achieve its objectives should be reported to those positioned to make corrections. Not only should reported deficiencies be investigated and corrected, but any underlying cause should be eliminated – don't just treat the symptoms, cure the patient.